REMARKS/ARGUMENTS

Claims 10, 28, 35, and 41 have been amended in accordance with the suggestions made by the Examiner in the Office Action of May 21, 2004.

With respect to the Examiner's objection under 37 C.F.R. 1.75 (c) to claim 12, claim 12 has been cancelled.

The Examiner has rejected claims 13-30 and 38-42 under 35 U.S.C. 102(b) as being anticipated by Ford et al. (U.S. Patent No. 5,481,613).

Claim 13 is to a key release method that might be implemented for example in a key release agent. The claim has been amended to specify that the method involves obtaining decryptor authorization logic stored externally to the decryptor with use of the key related information. On the basis of this, a decision is made as to whether or not to release the key. The specific steps of "locating decryptor authorization logic ..." and "deciding based on the decryptor information and the decryptor authorization logic..." recited in claim 13 are not taught in the cited reference. Rather, as detailed below in the obviousness discussion, the solution of Ford revolves around the inclusion of an ACD block with each key release request. In fact the ACD block always follows the encrypted data around. Applicant's solution eliminates the need to include the ACD block with each step of obtaining and decrypting a key cyphertext.

Similar arguments apply to dependent claims 14-28 and to claims 38-42. The Examiner is respectfully requested to withdraw the 35 U.S.C. 102(b) rejection of these claims.

The Examiner has also rejected claims 1-12 and 31-37 under 35 U.S.C. 103(a) as being unpatentable over Ford et al. upon the basis of obviousness. Of these, claims 12 and 34 have been cancelled.

The invention of Ford et al. utilizes an access controlled decryption block (ACD) in order to perform decyptor authorization. More specifically, referring to col. 5 line 25 of Ford, "...the encryptor generates ...a protected data construct called an ACD (access controlled decryption) block". Col. 6, line 20 reads "The ACD, on the other hand, is a data structure which accompanies an encrypted message as it traverses a computer system from an encrypting system

(encryptor) to a decrypting system (decryptor). This data structure, which is generated by the encrypting system, contains a statement of the access control criteria relating to the encryption plus key related data which will enable a key release agent to calculate the decryption key." Then, later, a decryptor "initiates a key-release request by sending the ACD block and R key id. to the KRA", see column 6, line 40.

In other words, the criteria used to determine whether or not to release the key form part of a key release request. In sharp contrast, applicant's invention involves generating key release requests that do not include an ACD block, and as such do not contain access control criteria. Rather, the key release request is used by the KRA to determine/obtain decryptor authorization logic to be applied. By not including the logic in the key release request, the size of the request can be reduced, and much more complex decryptor authorization logic can be applied. Also, the logic can be updated without needing to update each piece of encrypted data. To clarify this, claim 1 of the present application has been amended to include the limitation:

> "the key release request for use by the key release agent to locate decryptor authorization logic stored externally to the key release request that is to be applied in determining whether or not to release the decryption key;"

As such, the decision regarding permission for the decryptor to decrypt of the key ciphertext utilizes retrieval of information which is not in the ACD. Applicant submits therefore that Ford et al. simply does not disclose, teach, or suggest the feature that a process of authorization utilizes information retrieved from a location external to the ACD.

The Examiner has argued that it would be obvious to one of ordinary skill in the art to exclude the use of the specific data structure as the ACD, and replace it with another data structure that just provides key related information and not the additional information associated with the ACD. With respect, applicant has not replaced the ACD – something included in a key release request – with something else that provides a similar function. Rather, the ACD has been omitted entirely, and the key release agent must look up, externally to the key release request, decryptor authorization logic to apply in determining whether or not to release the key. This is a completely different approach to key release to that taught in Ford.

Further details of this inventive approach are recited in dependent claims 2 to 11, and similar arguments also apply to claims 33, and 35-37.

Claims 31 and 32 are to an administrative interface for defining the decryption authorization logic to be applied. The Examiner has presented arguments around an administrative interface for defining ACD blocks. As discussed, applicant's invention does not concern ACD blocks, but rather with defining decryptor authorization logic to be maintained externally to key cyphertexts that can then be accessed by key release agents. Claim 32 in particular recites that the authorization logic is stored by the administrative interface. For these reasons, the specific steps recited in claims 31 and 32 are not taught in the cited reference.

For at least the above reasons Applicant requests that the Examiner withdraw the 35 U.S.C. 103(a) rejections of claims 1-11, 31-33, and 35-37.

In view of the forgoing, early favorable consideration of this application is earnestly solicited.

Respectfully submitted,
GLENN LANGFORD ET AL

By _____
Allan Brett
Reg. No. 40,476
Smart & Biggar

Date: June 24, 2005
RAB:PDB:map
Ottawa, Ontario, Canada
Tel.: 613-232-2486